INSA1

INSA2

Improvements In, or Relating to, Electronic Badges

The present invention relates to a telecommunications system employing electronic security badges to provide temporary access to a computer system protected by firewalls, methods of providing temporary, controlled, access to a secure computer system, and an administration computer architecture for use with a telecommunications system employing electronic security badges.

INSA3

With modern data communications technology, it is frequently desirable to give a site visitor access to a secure computer system over electronic transmission systems. For example, it may be desirable to hold a conference, or virtual meeting, in cyberspace, which is hosted on a secure computer, to which general public access is denied for security reasons. In such a meeting, it may be necessary for a visitor to run applications software on the host computer. However, the person hosting such a meeting may well wish to limit a visitor's access to a certain set of the applications available on the host computer. If access to the host computer is given to a visitor, this will, to some extent, compromise the security of the host computer, unless special steps are taken to protect the host computer.

Existing systems for providing access to computers protected by firewalls are either inflexible and difficult for a visitor to use, or ineffective in terms of preserving the security of the home computer.

INSA4

The present invention makes an electronic visitor's badge available to a person visiting a host computer protected by firewalls, and solves the problem of providing flexible, user friendly, access without compromising security. The present invention permits persons located behind an address translating firewall, which only allows HTTP, to obtain controlled access to privileged data information without compromising data security. The badge establishes a reliable contact from which only trustworthy instructions will emanate, i.e. the instructions will only come from an approved and security cleared visitor.

Initial contact between a visitor and the host, i.e. an individual responsible

for operation of the host computer, is established via a telephone conversation over the PSTN. Visitor and host agree on a password, or code word. The code is added, possibly in encrypted form, to the source code of an electronic badge. The electronic badge may be a Java applet which is compiled and placed on a webserver protected by the password. When this "applet" is run via port 80, i.e. the port used for communication through a firewall, the code in the control server is correlated to the code presented by the badge, in other words, it does not matter that the firewall between visitor and host has changed the IP address.

The present invention can be used in any situation where individuals wish to work on a common computer and it is not possible to exchange hardware, but the individuals are able to recognize each others voices. The invention facilitates secure control of access to a secure computer facility via exchange of identity badges over the Internet.

The present invention strengthens the link between three security elements:

- voice recognition;
- knowledge of a password; and
- possession of an electronic badge - i.e. an applet

and manages a translating/masking firewall, via port 80.

According to a first aspect of the present invention, there is provided a telecommunications system adapted to act as a platform for electronic meetings, comprises a visitor's computer, an administration computer, an application computer, a firewall protecting said application computer and a transmission path over the Internet, characterised in that communications between said visitor's computer and said application computer are mediated by an electronic badge generated by said administration computer and operating on said visitor's computer.

Said administration computer and application computer may be realised on a single data processing machine.

Alternatively, said administration computer and application computer may be distinct data processing machines, and communications between said visitor's computer and said application computer may be controlled by a firewall located in said administration computer.

Said administration computer may be protected by a firewall.

Said electronic badge may be an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

Said list of access rights may permit access to one, or more, software applications.

Said applet may be adapted to run on said visitor's computer and cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

Said administration computer may include a control panel linked to a web server adapted to issue electronic badges.

Said administration computer may include a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

Said control server may be linked to a firewall protecting said application computer, and said database of access rules may be linked to said firewall protecting said application computer.

Access to said webserver may be controlled by a password protection means.

An electronic visitor's badge may be created from said control panel and deposited for collection on said webserver.

Said visitor's computer may download said electronic visitor's badge by accessing said web server and giving a password and visitor identification.

Access rights associated with said visitor's badge may be altered while said visitor computer is connected to said application computer.

Said visitor's badge may be adapted to self destruct on receipt of a signal from said control server.

According to a second aspect to the present invention, there is provided a method of establishing access for a visitor's computer to an application computer protected by a firewall generated by an administration computer, over the Internet, characterised by mediating communications between said visitor's computer and said application computer with an electronic badge generated on said administration computer and operating on said visitor's computer.

Said administration computer and said application computer may be realised on a single data processing machine.

Said administration computer and application computer may be realised as distinct data processing machines, and communications between said visitor's computer and said application computer may be controlled through a firewall located in said administration computer.

Said administration computer may be protected with a firewall.

Said electronic badge may be an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

Said list of access rights may permit access to one, or more, software

applications.

Said applet may run on said visitor's computer and cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

Said administration computer may include a control panel linked to a web server adapted to issue electronic badges.

The method may include the steps of:

- establishing a voice link over the PSTN between a person operating said visitor's computer, herein referred to as a visitor, and a person operating said administration computer, herein referred to as a host;
- said host establishing that said visitor has clearance to access said application computer, and
- assigning and communicating a password to said visitor over said voice link.

Said administration computer may include a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

Said control server may be linked to a firewall protecting said application computer, and said database of access rules may be linked to said firewall protecting said application computer.

Access to said webserver may be controlled by a password protection means.

Said host may create an electronic visitor's badge by actuation of said control panel and depositing said electronic visitor's badge, for collection by said visitor, on said webserver.

Said visitor may access said webserver over the Internet, giving said password, and downloading said electronic visitor's badge.

Said method may include the steps of:

- said visitor requesting access, while connected to said application computer, to a first software application, not pre-authorised on said electronic visitor's badge;

- said control panel giving an alarm condition;

- said host confirming over said voice link that said visitor has requested access to said first software application; and

- modifying the access rights associated with said electronic visitor's badge via said control panel.

Said visitor's badge may self destruct on receipt of a signal from said control server.

According to a third aspect of the present invention, there is provided an administration computer, for use with a telecommunications system adapted to act as a platform for electronic meetings, said administration computer having a firewall protecting an application computer, characterised in that said administration computer is adapted to create an electronic badge to mediate communications between a visitor's computer and said application computer.

Said administration computer and application computer may be realised on a single data processing machine.

Said administration computer and application computer may be distinct data processing machines.

Said administration computer may be protected by a firewall.

Said electronic badge may be an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

Said list of access rights may permit access to one, or more, software applications.

Said applet may be adapted to run on said visitor's computer and cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

Said administration computer may include a control panel linked to a web server adapted to issue electronic badges.

Said administration computer may include a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

Said control server may be linked to a firewall protecting said application computer, and said database of access rules may be linked to said firewall protecting said application computer.

Access to said webserver may be controlled by a password protection means.

An electronic visitor's badge may be created from said control panel and deposited for collection on said webserver.

Access rights associated with said visitor's badge may be altered while a visitor computer is connected to said application computer.

INSA5

Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 illustrates, in schematic form, an overview of a telecommunications system, according to the present invention.

Figure 2 illustrates, in greater detail, the administration computer and application computer of Figure 1.

Figure 3 illustrates, in greater detail, the participator computer of Figure 1.

The system of the present invention may include seven main components, namely:

- a control server, 6, see the accompanying drawings;
- a control panel, 4;
- a visitor's badge, in the form of an applet, 9;
- firewalls, 17, 24 and 7;
- a webserver, 5;
- a PSTN telephone link, 1,2 and 3; and
- applications software, 13, 14 and 15.

As illustrated in the accompanying drawings, a telecommunications system which supports secure communication between a visitor's, or participator's, computer, 8, and application, or host computer, 24, has an administration computer 19. The participator computer, 8, is linked via a firewall, 17, to the Internet 18, and thence through firewall, 24, to the administration computer 19. The administration computer, 19, includes a webserver, 5, for issuing visitor's badges in the form of Java applets, and is protected by a password recognition unit, 20. The administration computer includes a control panel, 4, which may take the form of a visual screen based interface, allowing an operator to control the administration computer and the issue of electronic badges. Each badge is in the form of an

applet which, when run on a visitor's computer, such as 8, includes a series of icons for a range of applications on the application computer, to which the visitor is given access rights by the electronic badge. In the case of the embodiment illustrated in the drawings, these applications include applications 13, 14, and 15 which might be MS-Netmeeting, Word 6, and Coral Draw 6.

The administration computer also includes a control server, 6, which controls a server, 16, carrying the access rules for the application computer, 34, and the firewall, 7, which protects the application computer. Access to the individual applications packages 13, 14, and 15, is controlled individually via the firewall, so that access may be granted to one, two, or all of applications 13 to 15, depending on the access rights granted to a given electronic visitor's badge. Access rights associated with an electronic badge may be altered during the course of a meeting, or conference, via the control panel and control server, giving true dynamic control.

In operation, a visitor and host speak to each other over the telephone link 1, 3, 2. They agree a password and the access rights the visitor will have. The host may identify the visitor by his/her voice, or by exchange of personal information, a PIN number, or the like. Once identification has been established to the satisfaction of the host, a password is issued orally to the visitor. The host then set ups an electronic visitor's badge for the host on the webserver 5, including the agreed password and the agreed access rights for the visitor. The electronic visitor's badge now resides on webserver 5 and awaits collection by the visitor.

The visitor can now set up a data link over the Internet to control server, 6 on a channel 24. It should be noted that the different communications channels 24, 35, 27,26 and 25 are labelled for easy identification in the drawings and may, in fact, represent a single communications link. The visitor is then requested to give her/his password, which is authenticated by the password protection unit 20, which, in turn, permits the electronic badge to be transmitted to the visitor's computer. On receipt by the visitor's computer, the electronic password, which as previously stated is a Java applet, runs on the visitor's computer. The electronic badge causes a number of icons to be displayed on the visitor's computer, 10, 11, and 12. By actuating the icons, the visitor obtains access via firewall 7, to the applications 13, 14 and 15

running on the application computer 34. The firewall operates to control the applications and data files to which the visitor can obtain access in accordance with the password instructions encoded in the electronic visitor's badge and the access rules held on server 16, all of which can be controlled via the control server 6, and control panel 4.

Although, as illustrated in the drawings, the administration computer, 19, and the application computer, 34, may be distinct data processing machines, it is also possible to realise both computers on a single data processing machine.

Consider the following scenario.

Two persons, a visitor and host, agree to hold a meeting over Internet. The host has, at his disposal, a computer system called the Control Lab Room System, and is prepared to host the meeting on this computer. On the telephone, the host and the visitor agree on the name and password for a visitor's badge which will then be created. The host sits by the control panel of the Control Lab Room System and creates this visitor's badge, and at this stage connects certain privileges to the badge. For example, the visitor will be allowed, on showing his/her badge, the right to use the MS-Netmeeting software available on the application computer. The visitor's badge is lodged on the webserver which belongs to the system. The visitor then draws and activates the badge via a special website, the reception. The name and password to get access to the badge are those which the host and the visitor have agreed on the telephone. The host will see when the badge has been activated, via the control panel and, if the host gives a receipt for the activation, the conference will commence. The visitor's badge has control codes which enable the visitor to request access to a range of functions available on the application computer, e.g. video, or a protected webserver. The host and the visitor start by using MS_Netmeeting. Since the host created the visitor's badge with rights for this equipment, it will start without any fresh intervention via the control panel.

After a while, however, the visitor wants to establish a connection with a video camera which shows the host's conference room. Before he/she has requested permission to do this, he/she starts his/her video client. When this

happens, the control panel displays an alarm message, which shows that a visitor is trying to use a function for which the visitor has not been granted access rights. The host now asks the visitor, via the telephone link, if the attempt emanated from the visitor and, on receipt of a positive response, allocates, via a simple button press, the visitor with the right to establish the connection.

Now, suppose a hacker, called Charlie, tries to get access to the same video channel. Earlier in the week Charlie had intercepted IP-traffic which contained a visitor's badge. However, when he tried to use the badge, the host immediately identified the badge as time expired, and immediately excluded him from the conference. This time Charlie tries to steal the visitor's video flow. He is stopped once again, this time because the control server of the Control Lab Room System does not succeed in communicating with the visitor's badge which all authorized visitors must have. This causes a new alarm to be given. If the visitor, via the telephone, does not affirm that he has just opened a new client session, and the host is not satisfied that this second session also belongs to the visitor, the host refuses connection. Furthermore, the host will ignore all inquiries from that source for the remainder of the conference. The rest of the conference turns out well and, at the end of the conference, the host withdraws the visitor's badge by means of the control server, via its channel to the badge, issuing an instruction to the badge to self destruct.

In slightly more technical detail the course of events can be explained as follows.

The firewall informs the control server of an attempt to establish a connection which, based on pre-existing rules, the status of the visitor's badge and user control from the control panel, accepts, or denies, the connection, by creating a rule for the firewall to follow for this and similar connection attempts.

The visitor's badge is the critical point. Because it is an applet, it must be shown in a webreader on the visitor's screen in order to execute. If it is clicked away, it stops executing, and with that ceases to be valid. The source code of the visitor's badge includes the visitor's identity, together with the time period(s) for

which it is valid. It must show this information to make the control server accept a connection from it and, implicitly, from the location from which a person attempts to access the application computer.

The control server is the hub of the system. The control server creates the visitor's badge in accordance with instructions received from the control panel and places the visitor's badge on the webserver as described above. When the badge has been drawn from the webserver, it establishes contact with the control server. If the badge is still active, all manipulations the host performs with the badge on the control panel are reflected on the badge at the visitor's computer, and vice verse. The control server also controls the firewall, which provides the security for the conference.

The firewall has a number of rules to follow, like all firewalls. The difference here is that the host can dynamically change these rules, based on:

- judgment of the telephone part of the conference; and
- the guarantee the visitor's badge gives about the identity of the person operating the computer connected through, or seeking connection through, the firewall.

The control panel gives the host a view of the whole system. All badges which have been distributed can be seen here, together with the functions that are active. All events which the host can influence in the system are shown on the control panel via the same interface as the visitor has, i.e. the badge.